CyberCIEGE™: An Information Assurance Teaching Tool for Training and Awareness

Cynthia E. Irvine, Michael F. Thompson
Naval Postgraduate School
irvine(thompson)@nps.edu

Ken Allen
Rivermind, Inc.
kallen@rivermind.com

Abstract

Good security is not intrusive and can be almost invisible to typical users, who are often unaware of or take it for granted. However, good security practice by user populations is a critical element of an organization's information assurance strategy. This is reflected in government information assurance teaching mandates such as DoD Directive 8570.1, which outlines objectives and requirements for information assurance (IA) education, training and awareness. Although mundane education, training and awareness programs may temporarily raise user interest, for many, mandatory education is considered a distracting waste of time. A new approach is needed to convey IA concepts that will engage the user's imagination.

CyberCIEGE[*+] *is an innovative computer-based tool to teach information assurance concepts. The tool enhances information assurance education and training through the use of computer gaming techniques. In the CyberCIEGE virtual world, students spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack.*

This paper describes CyberCIEGE and will present ways in which this tool can be used to achieve Federal and DoD information assurance teaching objectives.

[*] Development of CyberCIEGE was sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, and the Office of the Secretary of Defense. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.

[+] CyberCIEGE is a Trademark of Rivermind, Inc.

1 Introduction

On a typical day, a government employee may be made acutely aware of a wide array of security problems. With the first look at email in the morning a pile of spam and pfishing attempts fill the junk mail folder for perusal and disposal. The science section of the online newspaper describes new attacks and asks readers: "Is your wireless network secure?" Despite these constant reminders, the general population often takes a very nonchalant attitude toward securing information systems. Even within major organizations, users select trivial passwords and think that, so long as they keep their machines within viewing distance, arbitrary hookups to unknown wireless networks and to the Internet pose no threat. Thus, despite their increased awareness of security problems, users and administrators of systems continue to take few effective precautions. For many, the problems of cyber security appear so overwhelming that they choose to ignore it. This user apathy is mitigated through IA education.

Programs in information assurance (IA) awareness should cover several major areas. First, users should appreciate the impact of poor security choices on the health of the organization. Second, users should be provided with instruction that helps them understand the concrete steps they can take to improve cyber security within their organization. For a typical user, this may be as simple as understanding notions such as the value of a good password that is changed periodically. For a technologist, the effect of certain network topologies and connections on security might be addressed.

Recognizing the importance of IA user training and awareness, decision makers in the Federal Sector have mandated training and awareness

programs. For example, Department of Defense Directive 8570, Information Assurance Training, Certification, and Workforce Management [2], provides overarching policy regarding training and education in information assurance. In addition it assigns responsibilities to DoD components to ensure that this training is carried out. The policy states that "All authorized users of DoD IS shall receive initial IA awareness orientation as a condition of access and thereafter must complete annual IA refresher awareness." Responsibility for this training is allocated to the heads of DoD components.

A major challenge is the effective implementation of such programs. Too often, education and training in IA is mundane and boring for both users and administrators. In addition, certain critical conceptual issues often elude policy makers, whose perceptions are molded by hyperbolic news accounts. As in so many disciplines, effective information requires a tacit understanding of the art of security engineering. Thus IA training and education can benefit from an engaging presentation format that captures the user's imagination.

Interactive simulations show considerable promise as educational tools. By generating a sense of competition, these tools, which often appear to be games, that provide an exciting environment in which the participant has a stake in the outcome. For many learners, visualization associated with the activity can help to teach or re-enforce concepts.

In this paper, we describe CyberCIEGE, a simulation tool created by the Center for Information Systems Security Studies and Research at the Naval Postgraduate School and Rivermind, Inc. to teach IA concepts and practice.

2 Resource Management Simulations

CyberCIEGE [5], [3], [6] is a resource management simulation in which the user assumes the role of a decision maker for an IT-dependent organization. The objective is to keep the organization's virtual users happy and productive while providing the security measures needed to protect valuable organizational information assets. Within a given CyberCIEGE scenario, the user has a budget and must make choices regarding procedural, technical and physical security. With good choices the organization prospers and the scenario advances; poor choices often result in disaster. CyberCIEGE uses the potential tension between strong security and user productivity to illustrate that many security choices are an exercise in risk management.

The potential for resource simulation tools to capture a user's attention is illustrated by the success of games such as SimCity™ and RollerCoaster Tycoon®. In these games, players engage in planning and construction and observe the results of their choices. CyberCIEGE has a similar goal. The student is immersed in an environment where his or her choices have visible effects on the ability of virtual users to perform productive work and on the ability of attackers to compromise assets. Students build and configure networks of computers. The scenarios strive to give the user an emotional attachment to that which they have built, thereby providing a more acute learning experience when bad decisions lead to loss.

The tool includes several different scenarios, each of which is run separately. Each scenario includes a briefing that describes an enterprise (e.g., a business that manufactures bowling balls) and gives the player information about what must be done to help make the enterprise successful. Within each scenario, the enterprise has a defined set of users and assets. Users are typically employees of the enterprise whose productive work makes money for the enterprise. Assets are various kinds of information that users must access to be productive. Examples of assets are secret formulas, corporate accounting information, business plans, expense statements, and marketing material. Each enterprise has a number of different virtual users who each need to access different assets in different ways to be productive for the enterprise. These are *user goals*. And sometimes, assets need to be shared among users, who may also need to simultaneously access multiple different assets. Different assets have different secrecy, integrity and availability values, and different users have different authorizations to access assets as defined by the enterprise security policy.

Artwork, as shown in Figure 1, enhances the ambiance of each scenario.

Each scenario is characterized by predefined users, assets, user goals and an enterprise security policy. Once established, they are not subject to change by the student. What distinguishes CyberCIEGE is the limitless number of possible scenarios that can be created to teach IA.

3 Elements of CyberCIEGE

CyberCIEGE consists of several elements: a unique simulation engine, a scenario definition language, a scenario development tool, and a video-enhanced encyclopedia. CyberCIEGE is extensible in that new CyberCIEGE scenarios tailored to specific audiences and topics are easily created. Scenario-based event triggers are used to introduce new problems for the player to solve and to generate log entries for subsequent student assessment.

A major objective in the development of CyberCIEGE was to create a tool for which a large number of scenarios could be developed. This was motivated by two factors. First, information assurance is an enormous field. We concluded that many scenarios with different points of focus and depth of detail are needed to begin to cover the large number of IA topics. Some scenarios are lengthy and take hours to run, while others are short and focus on specific security concepts (e.g., password management). This allows IA educators to tailor scenarios for particular teaching objectives.

The second factor driving the creation of an extensible tool is to allow advanced students to create their own scenarios. Here, a student must make up an information security policy from whole cloth and imagine the kinds of tensions that could develop from trying to enforce the policy while letting users achieve their goals. This provides the potential for students to encounter

Figure 1: CyberCIEGE users at work

scenarios that cannot be won, e.g., due to information security policies that are not enforceable.

3.1 Simulation Engine

At its foundation, CyberCIEGE contains a sophisticated simulation engine, the Rivermind-proprietary TYBOLT game engine. TYBOLT is a multi-purpose PC- and next generation console-based engine designed for both games and simulations. At its heart is a multi-platform 3D graphics library. Anything from simple static objects to complex animated characters can be imported from industry standard tools, such as Maya [1], directly into the TYBOLT engine.

Another TYBOLT innovation is its 3D Graphical User Interface library. This library allows for the creation of Windows-like User Interfaces within a fully 3D environment.

The TYBOLT engine also contains: an Artificial Intelligence system, a video playback library, a sound library, a memory management system, a resource management system, and a real-time strategic/network/economic engine.

When targeting PC or XBOX applications, TYBOLT uses DirectX 9 [11] to insure the greatest possible compatibility with modern 3D video cards.

3.2 Scenario Definition Language

CyberCIEGE is built around a language that expresses security-related risk management tradeoffs for different scenarios. The CyberCIEGE simulation engine interprets this scenario definition language and presents the student with the resulting simulation. What the student experiences and the consequences of the player choices are a function of the scenario as expressed using the scenario definition language. The language includes the following major elements:

Assets: Information of some value to the enterprise. The virtual users access assets as part of achieving their asset goals. Examples of assets are secret formulas, corporate accounting information, business plans, expense statements, and marketing material. Some assets are of high value to the enterprise, while others are inconsequential. Thus there is a *cost* to the enterprise if the asset is compromised. Assets have different *motive values* to attackers, resulting in different levels of motivation for attacks against the assets. Some assets have value to attackers because they are secret (e.g., proprietary manufacturing data). Other assets have value because of their integrity (e.g., authoritative accounting records). Some assets have security labels, and the value of labeled assets is separately described. Thus a variety of assets can have a "Proprietary" label, and each asset with that label inherits the same cost and motive values. A given asset can have cost and motive values derived from a label as well as values explicitly tied to other users, i.e., to express discretionary security policies.

Users: Each CyberCiege scenario includes a set of virtual users whose productive work makes money for the enterprise. Users have work goals that must be met for the users to remain productive and happy. The student is responsible for providing the resources and environment needed by users to reach their goals. Each user has one or more goals expressed as a need to access specific assets. Some goals can express a rather abstract desire such as: "Joe wants to receive email from the Internet." Other goals express more detail such as: "Mary wants to use the Data Inversion Application software program to modify the secret sauce asset while reading the production schedule asset." Some user goals are correlated with that user's productivity. Other goals relate to a user's happiness (e.g., a desire to surf the Internet or get personal email). If a user fails to achieve productivity goals, it can directly affect the enterprise's bottom line. Failing to achieve a happiness goal does not directly affect the bottom line, but may eventually result in a disgruntled employee, which can ultimately impact enterprise security.

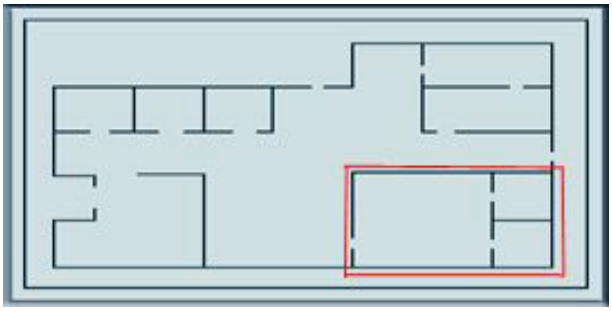

Figure 2: Office floor plan highlighting a zone

Zones: Each scenario includes one or more physical zones that can be used to control the physical movement of users. An example of a zone is a physically secure office with a locked door for which only selected users have a key. When IT components are purchased, they are placed within a specific zone. Physical access to components can therefore be constrained based on the physical access to the zone. As shown in Figure 2, the entire office is itself a zone, and it can contain additional zones to which additional security measures are applied.

Conditions and Triggers: The scenario designer defines conditions to be assessed by the engine during play, and specifies actions to occur as the result of a combination of conditions. For example, at some point in the simulation, a virtual user can receive a new asset goal, requiring the player to take actions to enable the user to achieve the goal. Or the scenario designer can cause specific types of attacks to occur (or not occur) depending on different conditions such as elapsed time and whether users are achieving goals. Player progress, hints and complaints from unhappy users can appear using pop-up windows and a moving message ticker at the bottom of the screen. Winning and losing are also defined using conditions and triggers. This allows the scenario designer to present the student with different debriefing screens dependent on the reason the game was lost.

Objectives and Phases: Scenarios can be divided into several phases, each consisting of one or more objectives. Objectives are defined in terms of conditions, as described above. The student must achieve each objective in a given phase before the simulation will transition to the next phase. This permits the scenario designer to guide the student through the scenario and gives the student an incremental sense of achievement.

3.3 Scenario Definition Tool

The Scenario Definition Language is sophisticated and syntactically demanding, requiring several thousand lines of text to express a full scenario. Scenario designers can use a forms-based scenario definition tool to construct scenarios without wrestling with the language syntax. This tool provides a development environment in which scenario designers can construct scenarios that employ re-usable libraries of scenario elements (e.g., groups of users, assets, etc.). This allows the easy construction of families of scenarios with only minor changes [7]. The development environment includes tools for compiling, validating, and running newly constructed scenarios as simulations. Figure 3 shows a typical screen from the Scenario Definition Tool.

CyberCIEGE has been designed so that a single scenario can be a well-defined information assurance teaching unit. Using the concept of a *campaign*, these teaching units may be combined to create a coherent succession of scenarios that provides either a succession of progressively more difficult scenarios or a focused training unit that covers several topics [13].

3.4 Encyclopedia

To complement the interactive virtual environment, CyberCIEGE contains an encyclopedia. At any time during a scenario a user can type the “e” or “E” key to invoke the

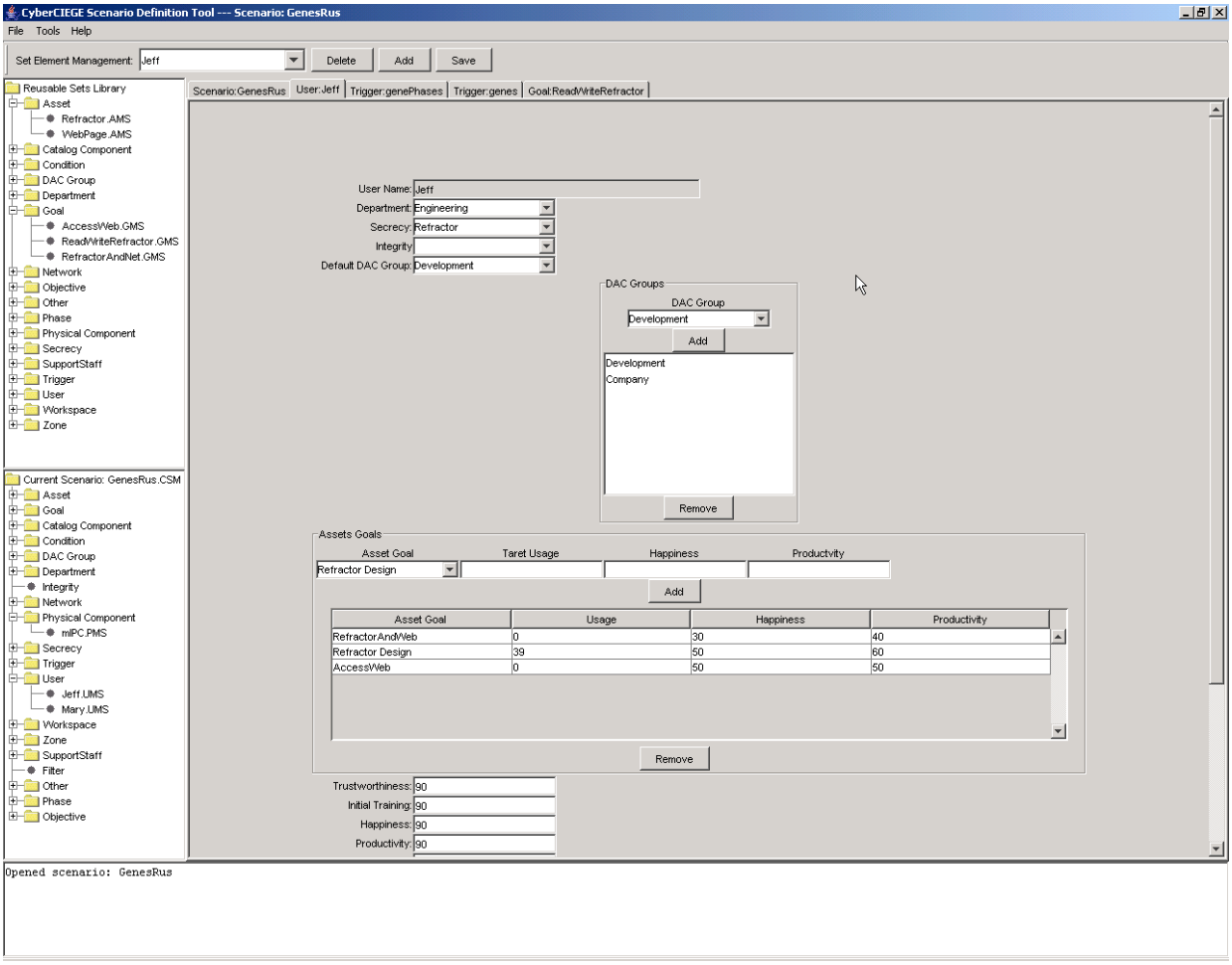

Figure 3: Scenario Definition Tool

encyclopedia. Here the user is presented with a menu leading to a variety of topics. There are encyclopedia entries that teach the student how to play the game. These include a description of the constants within scenarios and the elements of the scenario over which the user has control. Students can learn how to tell if they are winning or losing.

Another set of encyclopedia entries describes a broad range of information assurance topics. These include descriptions of policy, passwords, network security devices, malicious software, access control mechanisms, etc.

Since that not all users of CyberCIEGE may want to read even one page of an encyclopedia, a set of movies has been created to complement material in the encyclopedia. The movies are cartoons that describe security topics. They are intended to be understandable even by children and are designed to be entertaining to all age groups. The initial release of CyberCIEGE contains movies about security policy, malicious software, firewalls, and assurance. In addition, for users who may be new to computer-based simulations, a movie describing how to use CyberCIEGE is included.

4 CyberCIEGE Use

At the start of each scenario, the student is presented with a briefing that describes the scenario and the enterprise for which the student must manage computer resources. In some scenarios, the student is responsible for configuring existing computer components, including their connections to networks; making choices related to physical security and procedural security; and hiring information technology support staff. In other scenarios, the student is

also responsible for purchasing specific computer components and connecting them with networks. Players are advised of their limited budget for buying and maintaining equipment and hiring support staff.

The student's objective is to make money for the enterprise by efficiently and securely managing the enterprise computer networks. To succeed in a particular scenario, the student must understand each virtual user's needs to access different assets, i.e., the *user goals*. The student must then ensure that the users have suitable computer components, software, network interconnections and technical support personnel to achieve their goals of accessing assets.

The student must create and maintain an environment where the assets are protected in accordance with the enterprise security policy. The enterprise security policy is defined in terms of which virtual users are authorized to access which assets. Failure to adequately protect the assets results in monetary losses to the enterprise due to direct loss (e.g., stolen secret formulas), and lost user productivity (e.g., time lost reconstructing destroyed assets). The following kinds of choices affect the protection of assets in accordance with the security policy:

- Select components that enforce selected security policies and deploy the components in suitable topologies.
- Configure components to aid enforcement of the policies (e.g., automatic logoff after inactivity).
- Interconnect components using networks (or chose to not interconnect certain components).
- Instruct users to follow certain procedures (e.g., discourage them from picking dumb passwords) and provide users with adequate training.
- Impose physical security by limiting which users can enter a physical zone (e.g., a secure office area), and enforcing these limitations (e.g., armed guards, surveillance cameras, etc.)
- Perform selected degrees of background checks (e.g., criminal records, work history) on different kinds of users.

These security choices affect the protections provided to the enterprise assets, which are subject to attack from vandals, disgruntled employees, professional attackers, incompetent users and acts of nature. The most challenging attacks to protect against are from professionals that target specific assets. The means employed by professionals to compromise assets depend on the attacker motive, i.e., the value of the asset to the attacker.

Students can start and pause the simulation at any time. Typically, players are encouraged to construct networks and make policy enforcement decisions prior to starting the simulation. This is analogous to configuring and assessing a deployed system prior to taking it operational. After the student starts the simulation, virtual users may start creating and accessing their assets, and without due care, this may occur in ways that make the assets vulnerable to attack.

During the simulation, students can select and observe the status of a user's productivity and happiness. Users who cannot achieve their goals become agitated and pound on the keyboard. A message ticker at the bottom of the screen and pop-up messages can be used by scenario designers to inform students of their progress.

5 CyberCIEGE Status

Students at the Naval Postgraduate School developed a number of scenarios to test the simulation while it was under development [4], [8], [9], [10]. Additional scenarios were developed for the distribution version.

A limited distribution version of CyberCIEGE has been created and, in February 2005, was made available at no cost to agencies of the US Government. Concurrently, an evaluation version of the commercial product was made available by Rivermind. CyberCIEGE will be released by Rivermind in the spring of 2005.

The extensibility of CyberCIEGE offers an unparalleled opportunity for information assurance educators to contribute to its further growth. NPS has created a website for CyberCIEGE at http://cisr.nps.navy.mil/cyberciege.html. The site

contains information about the tool and provides contact information, such as the CyberCIEGE email address: cyberciege@nps.edu.

The web site is intended to provide a location where educators can share scenarios with others. Our model is taken from the open source community. New scenarios will be reviewed prior to posting on the web site to ensure appropriateness and quality control. Using this paradigm, an educator might add a relatively simple scenario about routers. A second educator could modify or add to that scenario perhaps by making the network configurations more complex. A third educator might extend the scenario further by establishing a more granular organizational policy. In this way a suite of scenarios would be available for others to download and use.

6 Comparison with Other Work

CyberProtect (http://iase.disa.mil/eta/index.html), an information assurance game created under the sponsorship of the Office of the Assistant Secretary of Defense for C3I and the IA Program Management Office of the Defense Information Systems Agency, is a resource management simulation of a relatively small, simple networked system with external connections to other parts of the organization as well as to the Internet. It provides students with a budget that is, by design insufficient to acquire all possible countermeasures, and requires them to select countermeasures to various IA threats. A probabilistic mechanism creates variations in game play. The game does not present the user with an organizational security policy. It is not immediately extensible by its users and instead is delivered with a fixed set of activities. In addition it does not present students with an engaging virtual world containing virtual people with goals and individual quirks.

Information Security Wargaming system (ISWS), which was created for the National Defense University, is a simulation that provides detailed insights related to particular attacks and defensive measures. The simulation is a tutorial that focuses on network-based attacks. A taxonomy of attacks has been developed and individual exercises focus on a particular type of attack in isolation. Given the organizational policy to be enforced, students select defensive tools to address the various phases of attack: protection, detection, assessment, recovery, and treatment. Feed back is provide as the simulation progresses and upon completion of the exercise. Unlike CyberCIEGE, this simulation is very abstract and static. No virtual world is presented where the impact of security choices is presented. In addition, this simulation contains a fixed number of scenarios.

Artificial Intelligence (AI) Wars: The Awakening [12] presents a three-dimensional futuristic world requiring strategy and actions. Players take on personae and enter the world of the computer, much in the manner of the 1982 Disney film TRON. It is designed purely for entertainment and does not present realistic information about various attacks or mitigating technologies.

7 Summary and Future Work

This section describes some future directions for CyberCIEGE and a brief summary.

7.1 Enhancements to the Current Tool

In the near term, NPS and Rivermind are seeking partner agencies interested in tailoring the tool to meet their specific IA teaching requirements. These partnerships might involve the development of new scenarios, creation of student assessment tools, extensions to the simulation, or new artwork. For example, an organization might want to create scenarios that included situations addressing privacy concerns in a highly networked IT environment.

An area for future research is that of teaching metrics and assessment. The Scenario Definition Language contains triggers that result in output to an activity log. Inspection of the log can indicate difficulties the student had while running the simulation and can be used to assess the student's understanding of the IA concepts presented. Like many auditing mechanisms, the activity log presents the instructor with information in a primitive format. To enhance the effectiveness of CyberCIEGE as a teaching tool, an assessment tool is needed.

The CyberCIEGE development team has focused on the creation of a factually correct and engaging tool. Its interfaces and artwork have been created by experienced members of the video game

community. Thus, the CyberCIEGE artwork and interfaces reflect common characteristics of video games. These games, and CyberCIEGE is no exception, present artwork that tends to be dark – danger lurks here. In addition, a high proportion of video game playing population is male. A study could be conducted to determine the appeal of the interface to users with different attributes, e.g. more mature students and female users. Further examination of human factors that might improve the teaching success of the tool among various populations could be explored.

7.2 Advanced CyberCIEGE Versions

Advanced versions of CyberCIEGE could take several forms among them, a wireless version and a multiplayer version.

7.2.1 Wireless Security

Mobile ad hoc wireless networks (MANETs) are decentralized and exhibit rapid changes in their topology. They are composed of elements such as laptops, PDAs, and other small devices that leave and enter the network unpredictably. At any moment each of these elements may be associated with a specific virtual user, a particular location, and certain assets. A given element may contribute to the enforcement of the enterprise security policy.

As more organizations move toward the use of mobile, wireless technology, new requirements for IA training and awareness will arise.

The current version of CyberCIEGE contains no mobile, wireless components. The overlay of such technology on the existing simulation would result in a significant advance in the ability of the tool to depict emerging network-centric architectures. New scenarios involving traveling virtual users, shared devices, and movable embedded systems would further extend IA education.

7.2.2 Multiplayer Version

Perhaps the most dramatic new development for CyberCIEGE would be its modification to make it a multiplayer game. In this form, students would have to protect and provide computer services to their virtual organizations while attempting to wage cyber attacks on competitors. The tool would be organized through the use of a substantially extended version of the scenario definition language. This would allow educators to steer users through various IA topics in a highly dynamic, competitive environment.

7.3 Summary

CyberCIEGE is an innovative computer-based tool to teach information assurance concepts. The tool enhances information assurance education and training through the use of computer gaming techniques.

As a tool that can be used to meet IA training and awareness goals, CyberCIEGE offers many advantages. It presents students with an engaging simulation. It is extensible: the scenario definition language and scenario definition tool support the creation of a limitless number of scenarios, which may be tailored to different educational venues.

Acknowledgements

We would like to thank Bill Chinn, Naomi Falby, Scott Gallardo, Brian Morgan, Matthew Rose, and Albert Wong, without whose dedication and talent CyberCIEGE could not have been created.

References

[1] Alias Systems Corp., Maya 6 Overview, http://www.alias.com/eng/products-services/maya/index.shtml
Last Accessed: 27 January 2005.

[2] Information Assurance Training, Certification, and Workforce Management, Department of Defense Directive Number 8570.1, August 15, 2004. http://www.dtic.mil/whs/directives/corres/pdf/d85701_081104/d85701p.pdf
Last Accessed: 27 January 2005

[3] Falby, N., Thompson, M. F., and Irvine, C. E., "A Security Simulation Game Scenario Definition Language," Innovative Program Abstracts - Colloquium on Information Systems Security Education, West Point, NY, June 2004.

[4] Fielk, Klaus W., CyberCIEGE Scenario Illustrating Integrity Risks to a Military-Like Facility, Masters Thesis, Naval Postgraduate School, Monterey, CA, September 2004.

[5] Irvine, C. E., and Thompson, M., "Teaching Objectives of a Simulation Game for Computer Security," Proceedings of Informing Science and Information Technology Joint Conference, Pori, Finland, June 2003

[6] Irvine, C. E., and Thompson, M., "Expressing An Information Security Policy Within A Security Simulation Game" Sixth Workshop on Education in Computer Security (WECS6), Monterey CA, July 2004. http://cisr.nps.navy.mil/downloads/WECS6_Proceedings.pdf
LastAccessed: 27 January 2005

[7] Johns, K. W. "Toward Managing and Automating CyberCIEGE Scenario Definition File Creation," Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2004.

[8] Lamorie, J. "A CyberCIEGE Scenario Illustrating Secrecy Issues in an Internal Corporate Network Connected to the Internet," Masters Thesis, Naval Postgraduate School, Monterey, CA, September 2004.

[9] LaMore, R. L. "CyberCIEGE Scenario Illustrating Secrecy Issues Through Mandatory and Discretionary Access Control Policies in a Multilevel Security Network," Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2004.

[10] Meyer, M. K. "A CyberCIEGE Scenario Illustrating Multilevel Secrecy Issues in an Air Operations Environment," Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2004.

[11] Microsoft, Corp. "Microsoft DirectX Technology Overview," http://www.microsoft.com/windows/directx/default.aspx
Last Accessed: 27 January 2005.

[12] Nexus Interactive. "AI Wars: The Awakening". http://www.aiwars.com/
Last Accessed: 27 January 2005

[13] Teo, T. L., "Scenario Selection and Student Selection Modules for CyberCIEGE", Masters Thesis, Naval Postgraduate School, Monterey, CA, December 2003.